Title: Computing singular elements modulo squares

Author: Przemysław Koprowski

Citation style: Koprowski Przemysław. (2020). Computing singular elements modulo squares. [Preprint]

COMPUTING SINGULAR ELEMENTS MODULO SQUARES

PRZEMYSŁAW KOPROWSKI

Abstract. The group of singular elements was first introduced by Helmut Hasse and later it has been studied by numerous authors including such well known mathematicians as: Cassels, Furtwängler, Hecke, Knebusch, Takagi and of course Hasse himself; to name just a few. The aim of the present paper is to present algorithms that explicitly construct groups of singular and S-singular elements (modulo squares) in a global function field.

1. Introduction

Let K be a global function field of odd characteristic and $\mathbb{F}_q$ be its full field of constants, where q is a power of an odd prime. The set of classes of discrete valuations on K can be viewed as a smooth complete curve X over $\mathbb{F}_q$. Assume that $\mathfrak{S}$ is a finite (possibly empty) subset of X. An element $\lambda \in K^\times$ is called $\mathfrak{S}$-*singular* if it has even valuations everywhere outside $\mathfrak{S}$. We denote

$$E_{\mathfrak{S}} = \{\lambda \in K^\times \mid \lambda \text{ is } \mathfrak{S}\text{-singular}\}$$

the group of $\mathfrak{S}$-singular elements of K. This group is a union of cosets of $K^{\times 2}$, hence we take a quotient group and denote it

$$\mathbb{E}_{\mathfrak{S}} := {}^{E_{\mathfrak{S}}}\!/_{K^{\times 2}} = \{\lambda \in {}^{K^\times}\!/_{K^{\times 2}} \mid \operatorname{ord}_{\mathfrak{p}} \lambda \equiv 0 \pmod 2 \text{ for } \mathfrak{p} \in X \setminus \mathfrak{S}\}.$$

If $\mathfrak{S}$ is empty we just write $\mathbb{E}$, rather than a bit awkward $\mathbb{E}_\emptyset$. In particular the group $E_{\mathfrak{S}}$ can be expressed as the extension of $\mathbb{E}_{\mathfrak{S}}$ by $K^{\times 2}$. The group $\mathbb{E}$ is sometimes called 2-*Selmer group* (see [1, 5, 9]). The quotient group $\mathbb{E}_{\mathfrak{S}}$ is a finite elementary 2-group, hence a finitely dimensional vector space over $\mathbb{F}_2$. As such it can be explicitly represented by its (finite) basis.

The aim of this paper is to present algorithms for constructing such bases. Of course, this problem is not completely new. For example, H. Cohen in [1] describes an algorithm for computing the group $\mathbb{E}$ in case when K is a *number* field. The main contribution of the present paper is twofold. First, we propose a use of auxiliary sets of places "compatible" (the term is explained later) with the constructed bases, that substantially simplify computation of coordinates of any given singular (respectively $\mathfrak{S}$-singular) element of $K^\times$ (see Propositions 2 and 6). Secondly, since computation of a Picard group may be a time consuming process, in Section 4 we introduce a randomized method for constructing singular elements without knowing the Picard group of X.

Throughout this paper we use the following notation: for a place $\mathfrak{p}$ of X by $\operatorname{ord}_{\mathfrak{p}}$ we denote the associated valuation. Observe that the parity of valuation is fixed throughout any given square class of K, hence we tend to treat $\operatorname{ord}_{\mathfrak{p}}$ as a function from ${}^{K^\times}\!/_{K^{\times 2}}$ to $\mathbb{Z}_2$. In addition, for $\lambda \in {}^{K^\times}\!/_{K^{\times 2}}$

by $\left(\frac{\lambda}{\mathfrak{p}}\right)$ we denote the natural generalization of the Legendre symbol to the whole square class group of K, that is

$$\left(\frac{\lambda}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \lambda \text{ is a square in } K_{\mathfrak{p}} \text{ (in particular } \operatorname{ord}_{\mathfrak{p}} \lambda \text{ is even)}, \\ 0 & \text{if } \operatorname{ord}_{\mathfrak{p}} \lambda \text{ is odd}, \\ -1 & \text{if } \operatorname{ord}_{\mathfrak{p}} \lambda \text{ is even but } \lambda \text{ is not a square in } K_{\mathfrak{p}}. \end{cases}$$

Next, for a divisor $\mathcal{D} \in \operatorname{Div} X$, by $[\mathcal{D}]$ we denote its class in the Picard group $\operatorname{Pic} X$ and by $\dim \mathcal{D}$ the dimension of the Riemann–Roch space $\mathcal{L}(\mathcal{D})$ of $\mathcal{D}$, where

$$\mathcal{L}(\mathcal{D}) := \left\{\lambda \in K \mid \operatorname{div}_X \lambda \geq -\mathcal{D}\right\} \cup \{0\}.$$

We will frequently use the fact that if G is an abelian group, then $G/2G$ has a natural structure of an $\mathbb{F}_2$-linear space. The dimension of this space is called the 2-rank of G and denoted $\operatorname{rk}_2 G$. Furthermore, when dealing with a finite set of places $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in X$, we will consider the cosets modulo $2 \operatorname{Pic} X$ of the classes $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_n] \in \operatorname{Pic} X$. In order to simplify wording, we shall write "$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are linearly independent (or form a basis) in $\operatorname{Pic} X/2 \operatorname{Pic} X$", meaning actually that these are the cosets modulo $2 \operatorname{Pic} X$ of their classes that are linearly independent (respectively form a basis) in $\operatorname{Pic} X/2 \operatorname{Pic} X$. We hope that the reader will excuse us this abuse of terminology, for sake of clarity of exposition.

The algorithms presented in this paper rely on some known procedures, like computation of the Riemann–Roch space of a divisor (see e.g. [7]) or construction of the Picard group of X (see e.g. [6, 8]). Moreover, we assume availability of standard linear algebra routines to deal with vector spaces over fields and lattices over $\mathbb{Z}$.

2. Group of singular elements

Let $\mathfrak{B} = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_n\} \subset X$ be a set of places and $\mathscr{B} := \{\beta_1, \ldots, \beta_n\} \subset \mathbb{E}$ be a set of square classes of singular elements. The two sets are said to be *compatible* if

$$\left(\frac{\beta_i}{\mathfrak{b}_i}\right) = -1 \qquad \text{and} \qquad \left(\frac{\beta_i}{\mathfrak{b}_j}\right) = 1$$

for all pairs of distinct indices $i, j \leq n$. In other words, β_i is a local square at all $\mathfrak{p}_j$ but $\mathfrak{p}_i$, where it is a non-square.

Proposition 1. *Let $\mathfrak{B} \subset X$ and $\mathscr{B} \subset \mathbb{E}$ be two compatible sets. The following conditions are equivalent:*

- *$\mathscr{B}$ is linearly independent in $\mathbb{E}$;*
- *$\mathfrak{B}$ is linearly independent in $\operatorname{Pic} X/2 \operatorname{Pic} X$.*

In particular, $\mathscr{B}$ is a basis of $\mathbb{E}$ if and only if $\mathfrak{B}$ is a basis of $\operatorname{Pic} X/2 \operatorname{Pic} X$.

For the proof of the proposition see [3, Section 3]. Using a pair of compatible bases has an evident advantage over working with a single basis. It is easy to get coordinates with respect to one basis from Legendre symbols computed against the other one. The following proposition is a special case of [3, Proposition 5].

Proposition 2. *Let $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{E}$ and $\mathfrak{B} = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_n\}$ be a compatible set of places.*

(1) *If $\lambda \in K^\times$ is a singular element, then its coordinates $\varepsilon_1, \dots, \varepsilon_n \in \{0,1\}$ with respect to $\mathscr{B}$ are given by a formula*

$$(-1)^{\varepsilon_i} = \left(\frac{\lambda}{\mathfrak{b}_i}\right), \qquad \text{for } i \in \{1, \dots, n\}.$$

(2) *If $\mathfrak{p} \in X$ is a place, then the coordinates $e_1, \dots, e_n \in \{0,1\}$ of $[\mathfrak{p}] + 2\operatorname{Pic} X$ in ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$ with respect to the basis $\mathfrak{B}$ satisfy the conditions*

$$(-1)^{e_j} = \left(\frac{\beta_j}{\mathfrak{p}}\right), \qquad \text{for } j \in \{1, \dots, n\}.$$

We may now present our first algorithm, that constructs a basis of the group of singular elements (modulo squares) from a compatible basis of ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$. Recall that a finitely generated abelian group G is presented in *Smith Normal Form* (SNF) if it is given as a direct sum of cyclic groups

$$G = C_1 \oplus \cdots \oplus C_k,$$

where the order of each C_i divides the order of its successors.

Algorithm 3. *Given a finite set $\mathfrak{B} = \{\mathfrak{b}_1, \dots, \mathfrak{b}_n\} \subset X$ of places that forms a basis of ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$, this algorithm constructs a compatible basis $\mathscr{B}$ of $\mathbb{E}$.*

1. *Initialize $\mathscr{A} := \{\zeta\}$, where $\zeta \in \mathbb{F}_q^\times$ is a non-square constant.*
2. *Let $\langle [\mathcal{D}_1] \rangle \oplus \cdots \oplus \langle [\mathcal{D}_m] \rangle$ be SNF presentation of $\operatorname{Pic}^0 X$, for some divisors $\mathcal{D}_1, \dots, \mathcal{D}_m$.*
3. *Find the minimal index $k \le m$ such that $[\mathcal{D}_k]$ has an even order or set $k := m+1$ if all the orders are odd.*
4. *For every index $i \in \{k, \dots, m\}$ proceed as follows:*
   (a) *Let d be be the order of $[\mathcal{D}_i]$ in $\operatorname{Pic}^0 X$.*
   (b) *Find a nonzero element α in the Riemann–Roch space $\mathcal{L}(d \cdot \mathcal{D}_i)$.*
   (c) *Append α to $\mathscr{A}$.*
5. *Using Proposition 2 for every element $\alpha_i \in \mathscr{A}$, $i \le n$ find its coordinates $\varepsilon_{i,1}, \dots, \varepsilon_{i,n} \in \mathbb{F}_2$ with respect to the sought basis $\mathscr{B}$ compatible with $\mathfrak{B}$.*
6. *Build a change of basis matrix $(e_{i,j}) := (\varepsilon_{i,j})^{-1}$.*
7. *Construct the basis $\mathscr{B} := \{\beta_1, \dots, \beta_n\}$ setting*

$$\beta_i := \alpha_1^{e_{i,1}} \cdots \alpha_n^{e_{i,n}}, \qquad \text{for } i \in \{1, \dots, n\}.$$

8. *Output $\mathscr{B}$*

Proof of correctness. The first part of the algorithm (steps 2–4) is nothing else but an adaptation of [1, Definition 5.2.7] to the case of function fields. On the other hand, steps 5–8 are just a standard change of basis. Thus, the correctness of the algorithm follows immediately from Propositions 1 and 2. □

Remark. Observe that the 2-rank of $\mathbb{E}$ equals the number of generators of $\operatorname{Pic}^0 X$ in SNF that have even orders. Therefore, when $\operatorname{Pic}^0 X$ has odd order, then k is set to $m+1$ and so the loop in step (4) is empty.

A general idea how to construct a basis of $\mathbb{E}$ is now clear. First we find a set $\mathfrak{B}$ of places whose classes form a basis of ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$, then we build a compatible basis $\mathscr{B}$. For sake of completeness let us write it down explicitly.

In the next algorithm we assume that we have a method for constructing a set of divisors whose classes generate $\operatorname{Pic} X$. Such an algorithm is described e.g. in [8].

Algorithm 4. *Given a global function field K, this algorithm constructs a basis (over $\mathbb{F}_2$) of the group $\mathbb{E}$ of singular elements modulo squares.*

1. *Find divisors $\mathcal{D}_1, \dots, \mathcal{D}_n$ whose classes generate* $\operatorname{Pic} X$.
2. *Find a set of indices $J \subset \{1, \dots, n\}$ such that the set $\{[\mathcal{D}_j] + 2\operatorname{Pic} X \mid j \in J\}$ generate the quotient group ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$.*
3. *Let $\{\mathfrak{p}_{j,1}, \dots, \mathfrak{p}_{j,k_j}\}$ be the support of $\mathcal{D}_j$ for every $j \in J$.*
4. *Using linear algebra find a maximal linearly independent (in ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$) subset $\mathfrak{B}$ of $\{\mathfrak{p}_{j,i} \mid j \in J, i \le k_j\}$.*
5. *Execute Algorithm 3 to construct a basis $\mathscr{B}$ compatible with $\mathfrak{B}$.*
6. *Output $\mathscr{B}$.*

Correctness of the above algorithm follows from the preceding discussion.

3. Group of $\mathfrak{S}$-singular elements

Now we turn our attention to a group of $\mathfrak{S}$-singular elements for some finite (generally nonempty) subset $\mathfrak{S} \subset X$. This task is substantially harder. We begin with a proposition describing the structure of the group $\mathbb{E}_{\mathfrak{S}}$.

Proposition 5. *Let $\mathscr{B} = \{\beta_1, \dots, \beta_n\}$ be a basis of $\mathbb{E}$ and $\mathfrak{B} = \{\mathfrak{b}_1, \dots, \mathfrak{b}_n\}$ a compatible set of places. Further let $\mathfrak{S} \subset X$ be a finite set disjoint with $\mathfrak{B}$ and $\mathfrak{S}' \subseteq \mathfrak{S}$ be a maximal subset of $\mathfrak{S}$ linearly independent in ${}^{\operatorname{Pic} X}\!/_{2\operatorname{Pic} X}$. Then:*

1. *For every place $\mathfrak{p} \in \mathfrak{S} \setminus \mathfrak{S}'$, there is a $\big(\mathfrak{S}' \cup \{\mathfrak{p}\}\big)$-singular element $\lambda_{\mathfrak{p}} \in K^\times$ such that*

$$\operatorname{ord}_{\mathfrak{p}} \lambda_{\mathfrak{p}} \equiv 1 \pmod 2 \qquad \text{and} \qquad \left(\frac{\lambda_{\mathfrak{p}}}{\mathfrak{b}}\right) = 1 \quad \text{for every } \mathfrak{b} \in \mathfrak{B}.$$

2. *The set $\mathscr{B} \cup \{\lambda_{\mathfrak{p}} \mid \mathfrak{p} \in \mathfrak{S} \setminus \mathfrak{S}'\}$ is a basis of $\mathbb{E}_{\mathfrak{S}}$.*

Proof. Without loss of generality we may assume that $\mathfrak{S}$ is not empty. If the classes of places in $\mathfrak{S}$ are linearly independent modulo $2\operatorname{Pic} X$, then $\mathfrak{S} = \mathfrak{S}'$, hence the first assertion holds vacuously and the second one is an immediate consequence of [2, Lemma 2.3], which says that in such case $\mathbb{E}_{\mathfrak{S}} = \mathbb{E}$.

Assume now that $\mathfrak{S}' = \{\mathfrak{s}_1, \dots, \mathfrak{s}_m\} \subsetneq \mathfrak{S}$ and fix a place $\mathfrak{p} \in \mathfrak{S} \setminus \mathfrak{S}'$. Then the coset of $[\mathfrak{p}]$ modulo $2\operatorname{Pic} X$ is a linear combination (over $\mathbb{F}_2$) of cosets of $\mathfrak{s}_1, \dots, \mathfrak{s}_m$. Hence there are: $\varepsilon_1, \dots, \varepsilon_m \in \{0, 1\}$, a divisor $\mathcal{D}$ and an element $\lambda \in K^\times$ such that

$$\operatorname{div}_X \lambda = \mathfrak{p} + \sum_{i \le m} \varepsilon_i \mathfrak{s}_i + 2\mathcal{D}.$$

It is then clear that $\operatorname{ord}_{\mathfrak{p}} \lambda \equiv 1 \pmod 2$ and λ is $\big(\mathfrak{S}' \cup \{\mathfrak{p}\}\big)$-singular. Set $\lambda_{\mathfrak{p}} := \lambda \cdot \beta_1^{e_1} \cdots \beta_n^{e_n}$, where $\left(\frac{\lambda}{\mathfrak{b}_i}\right) = (-1)^{e_i}$. Then $\lambda_{\mathfrak{p}}$ remains $\big(\mathfrak{S}' \cup \{\mathfrak{p}\}\big)$-singular since $\beta_1, \dots, \beta_n \in \mathbb{E}$. Moreover, $\lambda_{\mathfrak{p}}$ is a local square at each $\mathfrak{b}_i \in \mathfrak{B}$. This proves the first assertion.

In order to prove the second assertion let $\mathfrak{S} \setminus \mathfrak{S}' = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. Observe that the square classes of $\lambda_{\mathfrak{p}_1}, \dots, \lambda_{\mathfrak{p}_n}$ are linearly independent in ${}^{K^\times}\!/_{K^{\times 2}}$, since otherwise we would have $1 = \lambda_{\mathfrak{p}_1}^{e_1} \cdots \lambda_{\mathfrak{p}_n}^{e_n}$ for some $e_1, \dots, e_n \in \{0, 1\}$,

not all equal zero. But then 1 would have a nonzero valuation at some $\mathfrak{p}_i$, which is impossible.

On the other hand, any nontrivial element of the subgroup of $K^\times/K^{\times 2}$ generated by $\lambda_{\mathfrak{p}_1}, \dots, \lambda_{\mathfrak{p}_n}$ has an odd valuation at some $\mathfrak{p}_i$. Therefore this group intersects $\mathbb{E}$ only at $\{1\}$. Furthermore by [2, Lemma 2.3] we have $\operatorname{rk}_2 \mathbb{E} = \operatorname{rk}_2 \mathbb{E}_{\mathfrak{S}'}$. Thus [4, Lemma 2.5] together with [4, Proposition 2.3] yield

$$\begin{aligned}
\operatorname{rk}_2 \mathbb{E}_{\mathfrak{S}} &= \operatorname{rk}_2 \operatorname{Pic}(X \setminus \mathfrak{S}') + |\mathfrak{S}| \\
&\qquad - \operatorname{rk}_2 \operatorname{span}_{\mathbb{F}_2}\big\{[\mathfrak{p}]_{X\setminus\mathfrak{S}'} + 2\operatorname{Pic}(X\setminus\mathfrak{S}') \mid \mathfrak{p} \in \mathfrak{S}\setminus\mathfrak{S}'\big\} \\
&= (\operatorname{rk}_2 \mathbb{E}_{\mathfrak{S}'} - |\mathfrak{S}'|) + |\mathfrak{S}| - 0 \\
&= \operatorname{rk}_2 \mathbb{E} + |\mathfrak{S}\setminus\mathfrak{S}'| \\
&= \operatorname{rk}_2 \left(\mathbb{E} \oplus \operatorname{span}_{\mathbb{F}_2}\{\lambda_{\mathfrak{p}_1}, \dots, \lambda_{\mathfrak{p}_n}\}\right).
\end{aligned}$$

This proves that $\mathscr{B} \cup \{\lambda_{\mathfrak{p}} \mid \mathfrak{p} \in \mathfrak{S}\setminus\mathfrak{S}'\}$ is indeed a basis of $\mathbb{E}_{\mathfrak{S}}$. □

Proposition 6. *Keep the assumptions of the previous proposition and let* $\mathscr{A} := \{\beta_1, \dots, \beta_n\} \cup \{\lambda_1, \dots, \lambda_s\}$ *be the asserted basis of* $\mathbb{E}_{\mathfrak{S}}$. *If* $\mu \in K^\times$ *is* $\mathfrak{S}$*-singular, then its coordinates* $(\varepsilon_1, \dots, \varepsilon_n; e_1, \dots, e_s)$ *with respect to* $\mathscr{A}$ *satisfy the following conditions:*

$$(-1)^{\varepsilon_i} = \left(\frac{\mu}{\mathfrak{b}_i}\right) \qquad \text{and} \qquad e_j \equiv \operatorname{ord}_{\mathfrak{p}_j} \mu \pmod 2$$

for all $i \in \{1, \dots, n\}$ *and* $j \in \{1, \dots, s\}$

Proof. Write $\mu = \beta_1^{\varepsilon_1} \cdots \beta_n^{\varepsilon_n} \cdot \lambda_1^{e_1} \cdots \lambda_s^{e_s}$ and fix $j \le s$. Let $\mathfrak{p}_j \in \mathfrak{S}\setminus\mathfrak{S}'$ be the place corresponding to λ_j. Then λ_j is the only element among $\beta_1, \dots, \beta_n, \lambda_1, \dots, \lambda_s$ that has an odd valuation at $\mathfrak{p}_j$. Therefore

$$\operatorname{ord}_{\mathfrak{p}_j} \mu \equiv e_j \cdot \operatorname{ord}_{\mathfrak{p}_j} \lambda_j \equiv e_j \pmod 2.$$

Take now $\mu' := \mu \cdot \lambda_1^{e_1} \cdots \lambda_s^{e_s}$. Then μ' and $\beta_1^{\varepsilon_1} \cdots \beta_n^{\varepsilon_n}$ are in the same square-class. This means that μ' is singular and Proposition 2 says that its coordinates must satisfy the assertion. □

Now its time to forge the preceding propositions into actual algorithms. We begin with the one that constructs $\lambda_{\mathfrak{p}}$.

Algorithm 7. *Let* $\mathscr{B} = \{\beta_1, \dots, \beta_n\}$ *be a basis of* $\mathbb{E}$ *and* $\mathfrak{B} = \{\mathfrak{b}_1, \dots, \mathfrak{b}_n\}$ *a compatible set of places. Let* $\mathfrak{B}' := \{\mathfrak{b}_{n+1}, \dots, \mathfrak{b}_m\} \subset X$, $m \ge n$ *be an auxiliary set disjoint with* $\mathfrak{B}$ *and such that* $\mathfrak{B} \cup \mathfrak{B}'$ *generate the whole Picard group of* X. *Further, let* $\mathfrak{S}' = \{\mathfrak{s}_1, \dots, \mathfrak{s}_s\}$ *be a nonempty subset of* X *disjoint with* $\mathfrak{B} \cup \mathfrak{B}'$ *and linearly independent in* $\operatorname{Pic} X/2\operatorname{Pic} X$. *Given a place* $\mathfrak{p} \in X$ *such that* $[\mathfrak{p}] + 2\operatorname{Pic} X \in \operatorname{span}_{\mathbb{F}_2}\big\{[\mathfrak{s}_i] + 2\operatorname{Pic} X \mid i \le s\big\}$, *this algorithm finds an element* $\lambda_{\mathfrak{p}} \in K^\times$ *satisfying the first assertion of Proposition 5.*

1. *Use Proposition 2 to compute the coordinates of* $\mathfrak{p}$ *and* $\mathfrak{s}_1, \dots, \mathfrak{s}_s$ *with respect to the basis* $\mathfrak{B}$ *of* $\operatorname{Pic} X/2\operatorname{Pic} X$.
2. *Using linear algebra (over* $\mathbb{F}_2$*) find* $\varepsilon_1, \dots, \varepsilon_s \in \{0, 1\}$ *such that*
$$[\mathfrak{p}] \equiv \varepsilon_1[\mathfrak{s}_1] + \cdots + \varepsilon_s[\mathfrak{s}_s] \pmod{2\operatorname{Pic} X}.$$
3. *Select the subset* $\mathfrak{T} := \{\mathfrak{s}_i \mid \varepsilon_i = 1\} \subset \mathfrak{S}'$ *and let* $t := |\mathfrak{T}|$. *Denote the elements of* $\mathfrak{T}$ *by* $\mathfrak{t}_1, \dots, \mathfrak{t}_t$.

(4) *Take a lattice* $\mathbb{Z}^{1+t+m}$ *and a map* $\psi : \mathbb{Z}^{1+t+m} \to \operatorname{Pic} X$ *given by the formula*

$$\psi\big((v_0, \dots, v_t, v_{t+1}, \dots, v_{t+m})\big) := v_0[\mathfrak{p}] + \sum_{1\le i\le t} v_i[\mathfrak{t}_i] + \sum_{1\le i\le m} 2v_{t+i}[\mathfrak{b}_i].$$

(5) *Using linear algebra (over* $\mathbb{Z}$*) construct a sub-lattice* $V := \ker\psi$.
(6) *Find a vector* $v = (v_0, \dots, v_t) \in V$ *such that* $v_0 \equiv 1 \pmod 2$.
(7) *Let* λ *be a generator of the Riemann–Roch space*

$$\mathcal{L}\bigg(v_0\mathfrak{p} + \sum_{1\le i\le t} v_i\mathfrak{t}_i + \sum_{1\le i\le m} 2v_{t+i}\mathfrak{b}_i\bigg).$$

(8) *Set* $\lambda_{\mathfrak{p}} := \lambda \cdot \prod_{i\le n} \beta_i$, *where* $(-1)^{e_i} = \left(\frac{\lambda}{\mathfrak{b}_i}\right)$.
(9) *Output* $\lambda_{\mathfrak{p}}$.

Proof of correctness. Assume that $v = (v_0, \dots, v_{t+m})$ sits in the lattice V constructed in step (5). Then there is $\lambda_1 \in K^\times$ such that

$$\operatorname{div}_X \lambda_1 = v_0\mathfrak{p} + \sum_{1\le i\le t} v_i\mathfrak{t}_i + \sum_{1\le i\le m} 2v_{t+i}\mathfrak{b}_i.$$

In particular λ_1 is $\big(\mathfrak{T}\cup\{\mathfrak{p}\}\big)$-singular, so also $\big(\mathfrak{S}'\cup\{\mathfrak{p}\}\big)$-singular. We claim that V contains an element v with an odd first coordinate. Indeed, by assumption we have

$$[\mathfrak{p}] \equiv \sum_{i\le s} \varepsilon_i[\mathfrak{s}_i] = \sum_{i\le t}[\mathfrak{t}_i] \pmod{2\operatorname{Pic} X}.$$

Therefore, as in the proof of Proposition 5, there are: $\lambda_2 \in K^\times$ and $\mathcal{D} \in \operatorname{Div} X$ such that

$$\operatorname{div}_X \lambda_2 = \mathfrak{p} + \sum_{i\le t} \mathfrak{t}_i + 2\mathcal{D}.$$

By assumption, $\mathfrak{B}\cup\mathfrak{B}'$ generate the whole Picard group. Thus the class of $\mathcal{D}$ can be written as $[\mathcal{D}] = v_{t+1}[\mathfrak{b}_1] + \dots + v_{t+m}[\mathfrak{b}_m]$, for some integers $v_{t+1}, \dots, v_{t+m}$. This means that there is $\mu \in K^\times$ such that

$$\operatorname{div}_X \mu = -\mathcal{D} + \sum_{1\le i\le m} v_{t+i}\mathfrak{b}_i.$$

Consequently we obtain

$$\operatorname{div}_X(\lambda_2\mu^2) = (1 + 2\operatorname{ord}_{\mathfrak{p}}\mu)\cdot\mathfrak{p} + \sum_{1\le i\le t}(1 + 2\operatorname{ord}_{\mathfrak{t}_i}\mu)\cdot\mathfrak{t}_i + \sum_{1\le i\le m} 2v_{t+1}\mathfrak{b}_i$$

and trivially λ_2, $\lambda_2\mu^2$ are in the same square class.

Denote $\lambda := \lambda_2\mu^2$. By the preceding section, λ is $\big(\mathfrak{S}'\cup\{\mathfrak{p}\}\big)$-singular and it has an odd valuation at $\mathfrak{p}$. In particular

$$v = (\operatorname{ord}_{\mathfrak{p}}\lambda, \operatorname{ord}_{\mathfrak{t}_1}\lambda, \dots, \operatorname{ord}_{\mathfrak{t}_t}\lambda, \operatorname{ord}_{\mathfrak{b}_1}\lambda, \dots, \operatorname{ord}_{\mathfrak{b}_m}\lambda) \in V$$

has an odd first coordinate. This proves the claim

Now let $I \subset \{1, \dots, n\}$ be the set of these indices for which $\left(\frac{\lambda}{\mathfrak{b}_i}\right) = -1$. Then $\lambda_{\mathfrak{p}} := \lambda \cdot \prod_{i\in I} \beta_i$ remains to be $\big(\mathfrak{S}'\cup\{\mathfrak{p}\}\big)$-singular and has an odd valuation at $\mathfrak{p}$, but now it is a local square at every $\mathfrak{b} \in \mathfrak{B}$. Hence it is the element we are after. □

Remark. The set $\mathfrak{B}'$ appearing in the above algorithm may be possibly empty. It is so, when $\operatorname{Pic}^0 X$ can be decomposed into a direct sum of cyclic groups of even orders.

We are now ready to construct the group of $\mathfrak{S}$-singular elements. The correctness of the next algorithm follows from Proposition 5.

Algorithm 8. *Given a finite (possibly empty) set of places $\mathfrak{S} \subset X$, this algorithm constructs a basis (over $\mathbb{F}_2$) of the group $\mathbb{E}_{\mathfrak{S}}$ of $\mathfrak{S}$-singular singular elements modulo squares.*

1. *Find a basis $\mathfrak{B}$ of $\operatorname{Pic} X/2\operatorname{Pic} X$ disjoint with $\mathfrak{S}$ and a set $\mathfrak{B}' \subset X$ disjoint with $\mathfrak{B} \cup \mathfrak{S}$ and such that $\mathfrak{B} \cup \mathfrak{B}'$ generates $\operatorname{Pic} X$.*
2. *Use Algorithm 3 to construct a basis $\mathscr{B}$ of $\mathbb{E}$ compatible with $\mathfrak{B}$.*
3. *Use Proposition 2 to compute the coordinates with respect to $\mathfrak{B}$ of all $\mathfrak{s} \in \mathfrak{S}$.*
4. *Using these coordinates, find a maximal subset $\mathfrak{S}'$ of $\mathfrak{S}$ linearly independent in $\operatorname{Pic} X/2\operatorname{Pic} X$.*
5. *If $\mathfrak{S}' = \mathfrak{S}$ (in particular if $\mathfrak{S}$ is empty) output the basis $\mathscr{B}$ and terminate.*
6. *Denote $V := \operatorname{span}_{\mathbb{F}_2}\{[\mathfrak{s}] + 2\operatorname{Pic} X \mid \mathfrak{s} \in \mathfrak{S}'\}$ and $s := \dim V = |\mathfrak{S}'|$.*
7. *For every $\mathfrak{p} \in \mathfrak{S} \setminus \mathfrak{S}'$ do the following:*
   (a) *Find the coordinates $\varepsilon_1, \dots, \varepsilon_s \in \{0, 1\}$ of $\mathfrak{p}$ in V with respect to the basis $\mathfrak{S}'$.*
   (b) *Set $\mathfrak{T} := \{\mathfrak{s}_i \in \mathfrak{S}' \mid \varepsilon_i = 1\}$.*
   (c) *Execute Algorithm 7, but skip steps (1–3), and construct $\lambda_{\mathfrak{p}} \in K^\times$ that satisfies the first assertion of Proposition 5.*
8. *Output $\mathscr{B} \cup \mathscr{L}$, where $\mathscr{L} := \{\lambda_{\mathfrak{p}} \mid \lambda_{\mathfrak{p}} \in \mathfrak{S} \setminus \mathfrak{S}'\}$.*

4. Random generation of singular elements

Algorithms presented in the previous two sections rely on an explicit description of $\operatorname{Pic} X$. While algorithms that compute the Picard group are known and have been implemented in existing computer algebra systems, it is also known that the whole process can take considerable amount of time. If we need just one, random singular element of K, we may do better than construct the whole group $\mathbb{E}$.

Algorithm 9. *Given a global function field K, this algorithm constructs a random singular element of K.*

1. *Pick two random places $\mathfrak{p}, \mathfrak{q}$ of the same degree.*
2. *Find $k := \min\{j \geq 1 \mid \dim(j\mathfrak{p} - j\mathfrak{q}) \neq 0\}$.*
3. *If k is even, output a generator of the Riemann-Roch space $\mathcal{L}(k\mathfrak{p} - k\mathfrak{q})$ and terminate.*
4. *Otherwise, let $\zeta \in \mathbb{F}_q^\times$ be a non-square constant. Output at random (with probability $1/2$) either ζ or 1.*

Proof of correctness. By the finiteness of $\operatorname{Pic}^0 X$ (see [10, Proposition V.1.3]), the class of $\mathcal{D} := \mathfrak{p} - \mathfrak{q}$ is k-torsion for some positive integer k. Therefore $k \cdot \mathcal{D}$ is principal, while $i \cdot \mathcal{D}$ is not for any nonzero $i < k$. Hence there is $\beta \in K^\times$ such that $k \cdot \mathcal{D} = \operatorname{div}_X \beta$. In addition, β generates the Riemann–Roch space $\mathcal{L}(k \cdot \mathcal{D})$ since this space has dimension one by [10, Corollary 1.4.12]. We

claim that β is a singular element of K. Write the divisor $\operatorname{div}_X \beta$ of β in the form

$$\operatorname{div}_X \beta = m\mathfrak{p} + n\mathfrak{q} + \sum_{i \leq s} k_i \mathfrak{r}_i,$$

where $\mathfrak{r}_1, \ldots, \mathfrak{r}_s \in X$ are distinct from $\mathfrak{p}, \mathfrak{q}$. We have $\operatorname{div}_X \beta \geq -\mathcal{D} = k\mathfrak{q} - k\mathfrak{p}$. Therefore $m \geq -k$, $n \geq k$ and $k_i \geq 0$ for every index i. In particular, $\mathfrak{p}$ is the only pole of β. Furthermore, we have

$$0 = \deg(\operatorname{div}_X \beta) = m \cdot \deg \mathfrak{p} + n \cdot \deg \mathfrak{q} + \sum_{i \leq s} k_i \cdot \deg \mathfrak{r}_i.$$

From the fact that $\mathfrak{p}$ and $\mathfrak{q}$ have the same degree we infer that

$$-k \cdot \deg \mathfrak{p} \geq -n \cdot \deg \mathfrak{p} = -n \cdot \deg \mathfrak{q} = m \cdot \deg \mathfrak{p} + \sum_{i \leq s} k_i \cdot \deg \mathfrak{r}_i \geq m \cdot \deg \mathfrak{p}.$$

It follows that m equals $-k$. Consequently we obtain

$$\begin{aligned} 0 &= -k \cdot \deg \mathfrak{p} + n \cdot \deg \mathfrak{q} + \sum_{i \leq s} k_i \cdot \deg \mathfrak{r}_i \\ &= (n-k) \cdot \deg \mathfrak{q} + \sum_{i \leq s} k_i \cdot \deg \mathfrak{r}_i \geq (n-k) \cdot \deg \mathfrak{q} \geq 0. \end{aligned}$$

Thus we have $n = k$ and $\operatorname{div}_X \beta = k\mathfrak{q} - k\mathfrak{p} = -\mathcal{D}$. Hence $\operatorname{ord}_{\mathfrak{r}} \beta \equiv 0 \pmod 2$ for every $r \in X$, as claimed. □

It remains to analyze the distribution of elements of $\mathbb{E}$ produced by the algorithm. Unfortunately the distribution depends on the structure of the Picard group of X. (And in an actual implementation it is further impacted by the quality of the generator of random places of X.) Thus in general the distribution does not have to be uniform, unless $\operatorname{Pic}^0 X$ is an elementary 2-group.

Lemma 10. *Let G be a finite abelian group of a form $G = G_1 \oplus \cdots \oplus G_n$, where every G_i is cyclic of order $|G_i| = 2^{k_i} \cdot t_i$ with $2 \nmid t_i$. Let $g \in G$ be a random (uniformly distributed) element. The probability that the order of g is odd equals $2^{-(k_1 + \cdots + k_n)}$.*

Proof. Write g as $g = (g_1, \ldots, g_n)$ where $g_i \in G_i$. The order of g is odd if and only if the orders of all g_i are odd. Now, G_i is cyclic and $|G_i| = 2^{k_i} \cdot t_i$, hence G_i contains precisely t_i elements of odd order. Thus the probability that the order of g_i is odd equals 2^{-k_i} and consequently the probability that the order of g is odd equals $2^{-k_1} \cdots 2^{-k_n}$, as claimed. □

The group $\mathbb{E}$ can be expressed in a form $\{1, \zeta\} \oplus \mathbb{E}'$, where $\mathbb{E}'$ is a subgroup of $\mathbb{E}$. Thus, probability of random picking a constant singular element equals $2/|\mathbb{E}|$, provided that the distribution is uniform. The next corollary gives a partial answer to the question of the distribution of elements produced by Algorithm 9.

Corollary 11. *Probability that Algorithm 9 outputs a constant singular element (i.e. that step (4) gets executed) is less than or equal to $2/|\mathbb{E}|$.*

Proof. As in the proof of correctness of the algorithm, denote $\mathcal{D} := \mathfrak{p} - \mathfrak{q}$, where $\mathfrak{p}, \mathfrak{q}$ are two random points of the same degree. Recall that $\operatorname{Pic} X \cong \operatorname{Pic}^0 X \oplus \mathbb{Z}$, where the second coordinate of the class of a divisor is just its degree. It is a known consequence of Chebotarev density theorem, that classes of places of X, projected onto the first coordinate, are equidistributed in $\operatorname{Pic}^0 X$. Hence $[\mathcal{D}]$ may be any one of elements of $\operatorname{Pic}^0 X$ with equal probability. The preceding lemma asserts that the probability that $[\mathcal{D}]$ has an odd order cannot exceed $2^{-\operatorname{rk}_2 \operatorname{Pic}^0 X}$. Take a place $\mathfrak{o} \in X$ of odd degree. By [4, Proposition 2.3 and Lemma 2.6] we have

$$\operatorname{rk}_2 \operatorname{Pic}^0 X = \operatorname{rk}_2 \operatorname{Pic}(X \setminus \{\mathfrak{o}\}) = \operatorname{rk}_2 \mathbb{E}_{\{\mathfrak{o}\}} - 1 = \operatorname{rk}_2 \mathbb{E} - 1.$$

Consequently the probability of executing step (4) is bounded from above by the quantity

$$2^{-\operatorname{rk}_2 \operatorname{Pic}^0 X} = 2^{1-\operatorname{rk}_2 \mathbb{E}} = \frac{2}{|\mathbb{E}|}.$$

This proves the assertion. □

References

[1] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[2] Alfred Czogał a, Przemysł aw Koprowski, and Beata Rothkegel. Wild sets in global function fields. *Math. Slovaca*, 70(2):259–272, 2020.

[3] Alfred Czogała and Przemysław Koprowski. Graph of even points on an arithmetic curve. `https://arxiv.org/abs/1904.12177`.

[4] Alfred Czogała, Przemysław Koprowski, and Beata Rothkegel. Wild and even points in global function fields. *Colloq. Math.*, 154(2):275–294, 2018.

[5] David S. Dummit and John Voight. The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units. *Proc. Lond. Math. Soc. (3)*, 117(4):682–726, 2018.

[6] Florian Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. PhD thesis, Technische Universität Berlin, 1999.

[7] Florian Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[8] Florian Hess. Computing relations in divisor class groups of algebraic curves over finite fields. preprint `http://www.staff.uni-oldenburg.de/florian.hess/publications/dlog.pdf`, 2007.

[9] Franz Lemmermeyer. Selmer groups and quadratic reciprocity. *Abh. Math. Sem. Univ. Hamburg*, 76:279–293, 2006.

[10] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

Institute of Mathematics, University of Silesia, Bankowa 14, 40-007 Katowice, Poland

E-mail address: `przemyslaw.koprowski@us.edu.pl`